FAIL SAFE MEMORY

工学研究科 電気工学専攻
博士課程 3年次生
向殿政男
MUKAIDONO Masao

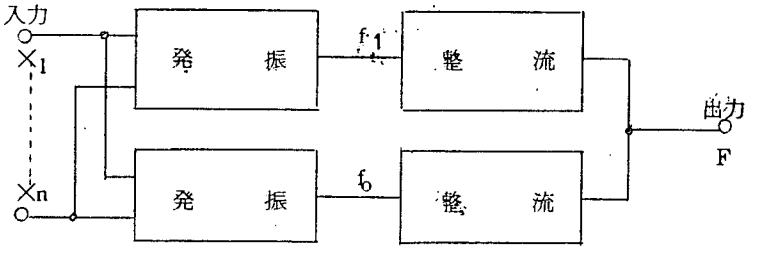
I まえがき

FAIL SAFE 論理回路について多くのアイディアが示され，実際の回路についてもいくつか製作されている。[※1]"決して真理値1には誤まらないFAIL SAFE論理回路"の構成法[※2]およびその応用[※3~4]についても本誌で述べた。FAIL SAFE論理回路として"決っして真理値1には誤まらない"という条件は必ずしも満足すべきものとはいえない。FAIL SAFE論理回路が満すべき理想的な条件は"正常に動作しているときは出力として真理値0または1を出し，もし回路内に故障が生じたときは出力として故障の状態（これを真理値$\frac{1}{2}$とする）をさし示めすこと"である。実際，このようなFAIL SAFE論理回路は構成可能[※1]なのである。また，このFAIL SAFE論理回路に，入力のうち1つでも$\frac{1}{2}$（故障入力）があれば出力は常に$\frac{1}{2}$となり，それ以外は0かまたは1となるような機能をもたせることも可能である。著者らはこのような3値論理回路の理論的研究も行なった。[※5]

本報告では，以上のFAIL SAFE 3値論理回路を用いたMEMORYについて考察する。

II 3値を用いたFAIL SAFE論理回路

論理回路の出力は，通常，真理値として0と1を有している。いま，真理値0に電圧0〔V〕を，真理値1に電圧V〔V〕を対応させたとする。論理回路をトランジスタなどで構成すると，多くの場合，切断，短絡などの故障により，出力が0〔V〕であるべきときV〔V〕になったり，逆に，V〔V〕であるべきとき0〔V〕になったりする可能性がある。これではFAIL SAFE論理回路にならない。そこで，真理値0に電圧$-V$〔V〕を，真理値1に$+V$〔V〕を対応させ，その中間の電圧$-V<v<+V$なるvに故障出力を表わす$\frac{1}{2}$を対応させる。そして，出力が1を出すべきとき発振する回路f_1と，0を出すべきとき発振する回路f_0をもうけて，これらの発振出力を整流してそれぞれ$+V$〔V〕，$-V$〔V〕とする（第1図参照）。このよ



第1図 FAIL SAFE 論理回路

うにすると，発振回路や整流回路などあらゆる部分の故障は出力電圧0〔V〕の方向であり，故障すれば出力は必ず$\frac{1}{2}$となる。すなわち，真理値0を出すべきとき故障により真理値1になったり，逆に1であるべきとき0になることは決ってしてなく，故障のときは必ず$\frac{1}{2}$となり理想的なＦＡＩＬ　ＳＡＦＥ論理回路が構成できる。

任意の論理関数はＡＮＤ(・)ＯＲ(∨)NOT(～)により構成できることが知られているからＦＡＩＬ　ＳＡＦＥなＡＮＤ，ＯＲ，ＮＯＴ回路を構成しよう。ここで，入力に$\frac{1}{2}$があるとき－前の段までの回路に故障があることを示している－，出力の値の割り当て方に二つある。一つは，

$$X \cdot Y = \min(X, X)$$

$$X \vee Y = \max(X, X)$$

$$\sim X = 1 - X$$

により出力を割り当てるもので，これらの真理値表は第1表～第3表となる（演算・，∨，～を有限回ほどこして得られる論理関数はＢ－３値論理関数といわれる）。

X ＼ Y	0	$\frac{1}{2}$	1
0	0	0	0
$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

第1表　X・Ｙ真理値表

X ＼ Y	0	$\frac{1}{2}$	1
0	0	$\frac{1}{2}$	1
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
1	1	1	1

第2表　Ｘ∨Ｙ真理値表

X	0	$\frac{1}{2}$	1
	1	$\frac{1}{2}$	0

第3表　～Ｘ真理値表

他の1つの方法は，入力に$\frac{1}{2}$が1つでもあれば出力を必ず$\frac{1}{2}$とするもので，ＮＯＴについては前者と同じであるが，ＡＮＤ，ＯＲについての真理値表は第4表，第5表となる（これを記号⊙，⋁で表わす。演算⊙，⋁，～を有限回ほどこして得られる論理関数はＣ形論理関数といわれる。

X ＼ Y	0	$\frac{1}{2}$	1
0	0	$\frac{1}{2}$	0
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

第4表　Ｘ⊙Ｙ真理値表

X ＼ Y	0	$\frac{1}{2}$	1
0	0	$\frac{1}{2}$	1
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

第5表　Ｘ⋁Ｙ　真理値表

一方，ＦＡＩＬ　ＳＡＦＥ論理回路に用いられる発振回路には次の3種類がある。

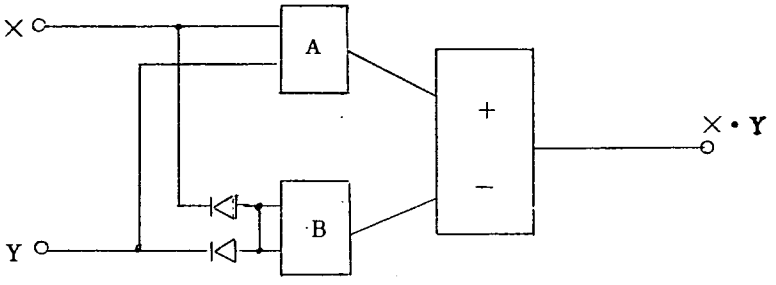
(i)　発振要素Ａ：全入力とも＋Ｖ〔Ｖ〕のときのみ発振。

(ii)　発振要素Ｂ：全入力とも－Ｖ〔Ｖ〕のときの発振。

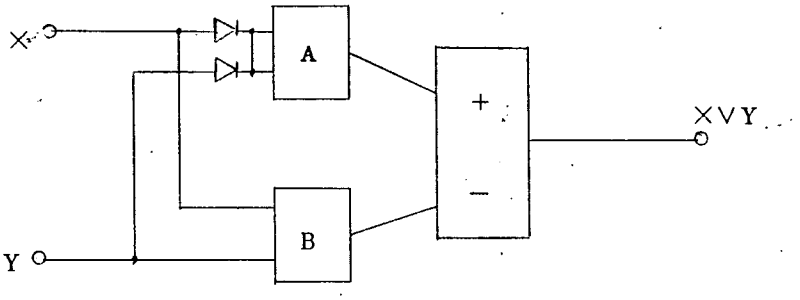
(iii)　発振要素ＡＢ：一方が＋Ｖ〔Ｖ〕，他方が－Ｖ〔Ｖ〕のときのみ発振。

以上の要素を用いて第1表，第2表，第4表，第5表を満すＦＡＩＬ　ＳＡＦＥ回路はそれぞれ第2図，

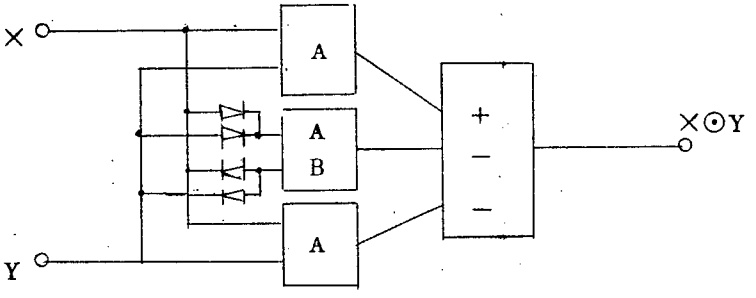
第3図，第4図，第5図のように図示される。図で，A，B，ABは上で述べた発振要素を表わし，＋，－と記してあるのは，発振出力を整流回路でそれぞれ＋V〔V〕，－V〔V〕に整流することを表わしている。



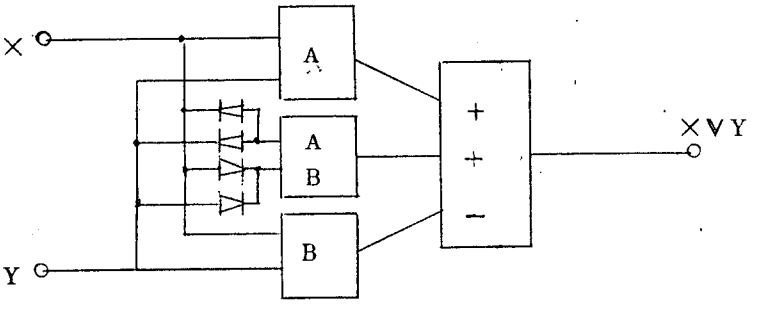
第 2 図　X・Y　構　成　図



第 3 図　X∨Y　構　成　図



第 4 図　X⊙Y　構　成　図



第 5 図　X∨Y　構　成　図

Ⅲ FAIL SAFEなFLIP−FLOP

ＭＥＭＯＲＹはもっとも簡単な順序回路である。論理回路を用いて構成されるＭＥＭＯＲＹについて考察する。まず，Ｓ－Ｒ ＦＬＩＰ－ＦＬＯＰ（以後Ｆ－Ｆと略記する）を考える。Ｓｅｔ 入力信号をＳ，Ｒｅｓｔ 入力信号をＲ，Ｆ－Ｆの出力信号をＦで表わし，各信号のとる値を０または１とするとＦ－Ｆの状態表は第６表のようになる。この表で，$t=\tau$ におけるＦの値を縦に，入力Ｒ，Ｓの値を横にとり，表中に表わされている値は $t=\tau+1$ におけるＦの値を表わしている。ここで，値を○印で囲んだところは安定点を示し，矢印で遷移の方向を示した。また？印はＦ（$\tau+1$）の出力が未定なところで，通常，Ｓｅｔ入力Ｒｅｓｅｔ入力が同時に１になることはないから，この値は自由に選んでよい。第６表で，？印の値を０ととるとＦ－Ｆは

F \ S \ R	1	0	0	1
0	⓪	⓪	1	?
1	0	①	①	?

第６表　Ｆ（$\tau+1$）の出力

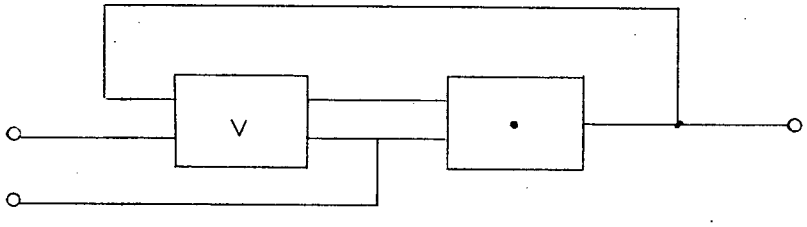
$$F(\tau+1)\rightleftarrows\sim R(\tau)\cdot\{S(\tau)\vee F(\tau)\}\cdots(1)$$

で表現される。前章で定義されたＦＡＩＬ　ＳＡＦＥなＡＮＤ(・)，ＯＲ(∨)，ＮＯＴ（～）回路を用いて第６図に示すようにＦＡＩＬ ＳＡＦＥなＦ－Ｆが実現される。(1)式を以後

$$F'\rightleftarrows\sim R(S\vee F)\cdots\cdots(2)$$

で表わすことにする。

次に，Ｃ形の順序回路，すなわち，入力のうち１つでも$\frac{1}{2}$がある場合，出力は必ず$\frac{1}{2}$となるような順序回路を構成しよう。組合せ回路の場合は，ＡＮＤ(・)，ＯＲ(∨)回路を各々第４表，第５表を満すＣ形のＡＮＤ(⊙)，ＯＲ(⩛)で置き換えれば，Ｃ形の組合せ回路を構成することができる。しかし，順序回路の場合はこうはならない。なぜならば，順序回路の場合は必ず ｆｅｅｄ－ｂａｃｋ ｌｏｏｐ が存在する。また，初期状態ではすべての回路の出力は$\frac{1}{2}$であり，これが入力に ｆｅｅｄ－ｂａｃｋ しており，$\frac{1}{2}$の入力信号が必ず存在することになる。もし，すべての論理回路が⊙⩛，～のみで構成されている場合には，どのような入力信号の組合せに対してもこの順序回路の出力を$\frac{1}{2}$以外の値にすることはできないことになる。すなわち，この順序回路は駆動できない。ここではまず，演算・，∨，～ のみの組合せでＣ形の順序回路を構成してみよう。一般に，順序回路は



第６図　　Ｆ　－　Ｆ

$$F' \rightleftarrows f(X_1, \cdots\cdots, X_n, F) \quad \cdots\cdots\cdots\cdots\cdots\cdots \quad (3)$$

で表わされる。ただし X_i ($i = 1, \cdots\cdots, n$) は入力を表わす。(3)式で，入力信号 X_i ($i = 1, \cdots, n$) のうち1つでも $\frac{1}{2}$ があるとき $F' \rightleftarrows \frac{1}{2}$ となり，それ以外のときは(3)式と等しい関数の1つに

$$F' \rightleftarrows f(X_1, \cdots\cdots, X_n, F) \vee \bigvee_{i=1}^{n} (X_i \cdot \sim X_i) \quad \cdots\cdots \quad (4)$$

がある。たゞし，f は加法標準形で表現されているとする。※6 これを(2)式に適用してみると，

$$F' \rightleftarrows \sim R\,S \vee \sim R \sim S\,F \vee \sim R \cdot R \vee \sim S \cdot S \quad \cdots\cdots\cdots \quad (5)$$

となり，RまたはSのうち1つでも $\frac{1}{2}$ が存在すると F' は必ず $\frac{1}{2}$ になる。(5)式の状態表は第7表のようになる。同図で※印のところは $F \rightleftarrows \frac{1}{2}$ の初期状態のとき，この順序回路を駆動することができるところを示している。すなわち，※印のついた列の入力R，Sの組み合せのとき，$F \rightleftarrows \frac{1}{2}$ から脱出できる。もし，(3)式で $F \rightleftarrows \frac{1}{2}$ としたとき，常に(3)式が $\frac{1}{2}$ ならばこの順序回路は駆動することができないのは，⊙，∨，～のみで順序回路を組んだときと同様である。

R \ S / F	0	$\frac{1}{2}$	1	0	$\frac{1}{2}$	1	0	$\frac{1}{2}$	1
0	⓪	$\frac{1}{2}$	⓪	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1	$\frac{1}{2}$	⓪
$\frac{1}{2}$	(1/2)	(1/2)	0※	(1/2)	(1/2)	(1/2)	1※	(1/2)	0※
1	①	$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	①	$\frac{1}{2}$	0

第7表　　F － F　状態表

ところで，(5)式で表わされる順序回路は実際にはあまり好のましくない。なぜならば，この回路にはハザードが存在して誤動作を起こさせる可能性を含んでいるからである。・，∨，～の回路の組合せで順序回路を組む場合，各回路の時間遅れはそれぞれ異なっていると考えなければならない。そのような場合，各変数が $\frac{1}{2}$ となったとき出力が $\frac{1}{2}$ となるのは，その回路系内にハザードが存在するのと同じ条件なのである。※※ よって，一般的に，(4)式でC形の順序回路を構成することは好のましくない。そこで，第7表の状態表を満足し，しかもハザードの存在しないFAIL　SAFEなF－Fを，前述した発振要素A，B，ABを用いて構成してみよう。第1図，f_1，f_0 を発振しているとき1，していないとき0を表わす関数とする。このとき，

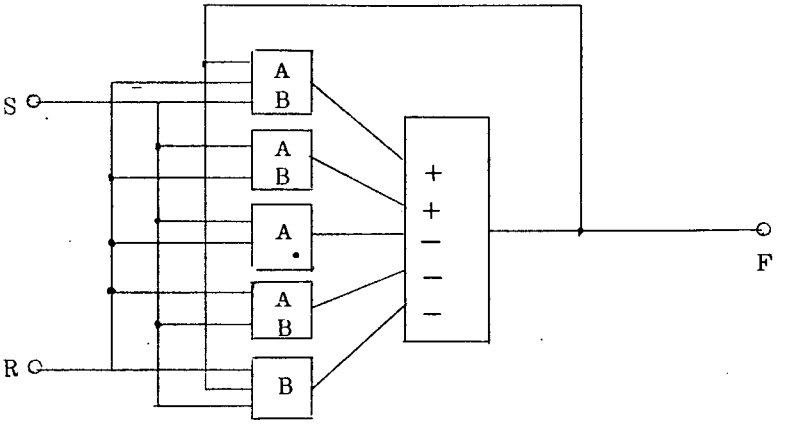
$$f_1 \rightleftarrows \delta_1 (\sim R \cdot S \vee \sim R \sim S \cdot F) \quad \cdots\cdots\cdots\cdots\cdots\cdots \quad (6)$$

$$f_0 \rightleftarrows \delta_1 (R \cdot S \vee R \cdot \sim S \vee \sim R \cdot \sim S \cdot \sim F) \quad \cdots\cdots\cdots\cdots\cdots \quad (7)$$

とすると，この回路は第7表の状態表を満足することは容易に示される。これは，各発振要素を用いると第7図のように構成できる。この回路では，前の場合のように各回路の時間遅れはないからハザードは存在しなく，前に述べたと同じ理由によりFAIL　SAFEになっている。ただし，入力R，Sは（出力Fに関してはかまわない）すみやかに0と1の間を変化しなければならない。0と1の変化の途中長い間

脚注　※※　証明は略す。詳しいことは改めて別に報告する予定である。

$\frac{1}{2}$でとどまっていると，それは故障入力とみなしてF－Fは故障出力$\frac{1}{2}$を出してしまう（これは，入力がいったん故障して，しばらく後に正常に回復したような場合と考えられる）。許されるこの時間巾はもちろん回路の特性により定まる。以上により，この回路は，非常に厳密な意味でのC形の順序回路を形成しているといい得る。



第　7　図

Ⅳ　特殊なＭＥＭＯＲＹについて

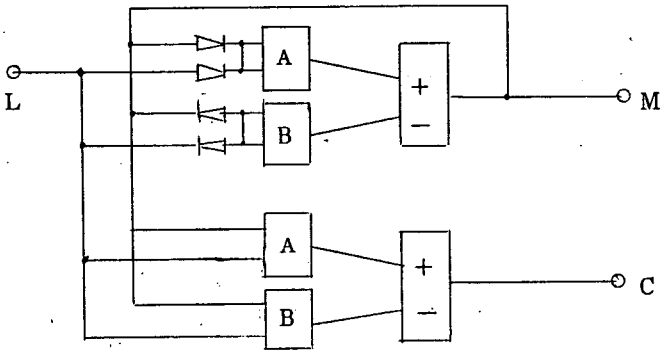
前章で考察したＦＡＩＬ　ＳＡＦＥなＭＥＭＯＲＹは，実際の計算機のＲＥＧＩＳＴＥＲなどに用いる場合には不適当と思われる。なぜならば，常に０→１，１→０の変化の途中で$\frac{1}{2}$をとる時間を短かく保つ事はむづかしく，また，実際問題として余り経済的であるとは思われない。

一方，非同期式計算機は次のような思想で設計されるのが望ましい。すなわち，計算機が動作する前はすべての論理回路の出力は$\frac{1}{2}$で，計算を開始すると０，１という情報が伝ばんして行き，最終出力が０または１になったことを検出することにより計算の終了を確認する。計算の終了を確認してから入力信号を$\frac{1}{2}$にもどし，最終出力が$\frac{1}{2}$にもどったことを確認してから次の計算を再び開始する。ところが，今迄の非同期方式計算機では計算の開始前ではすべての回路の出力を０にセットしておき，１という情報を伝ばんさせている。これでは０なる情報はセット時の０なのか情報の０なのか区別できない。これを区別するためには上に述べたように，まだ情報が伝わっていないことを表わす真理値$\frac{1}{2}$を持った３値論理回路を用いなければならない。もし，この非同期式計算機をⅡ章で述べたＦＡＩＬ　ＳＡＦＥな論理回路で組めば，真理値$\frac{1}{2}$は故障の状態，または情報がまだ伝達されていないことを表わしており，非常に好都合である。ところが，その為にはＭＥＭＯＲＹは入力が$\frac{1}{2}$になっても情報０または１を記憶していなければならず，前記のＭＥＭＯＲＹは使用できない。そこで，次のような特殊なＭＥＭＯＲＹを考える。すなわち，ＭＥＭＯＲＹの入力Ｉは通常$\frac{1}{2}$で，Ｉが$\frac{1}{2}$→１→$\frac{1}{2}$と変化することによりＭＥＭＯＲＹの出力Ｍは１を記憶し，$\frac{1}{2}$→０→$\frac{1}{2}$という変化で０を記憶する。このようなＭＥＭＯＲＹの状態表は第８表となる。この状態表を満足するＦＡＩＬ　ＳＡＦＥなＭＥＭＯＲＹは，発振要素Ａ，Ｂと整流回路を用いると第８図のように構成

することができる。前述したように，発振要素A，Bや整流回路の故障は出力が$\frac{1}{2}$の方向である。ただし，I＝1，M＝0　および I＝0，M＝1　のとき，発振要素A，Bの両方が発振し整流回路で加算されてMは$\frac{1}{2}$に遷移する訳だが，このとき回路の故障（断線）により遷移しない可能性がある。そこで第8図のように CHECK　回路Cをもうける。この回路の真理値表を第9表に示す。このように構成するとき，MEMORYの入力Iが0または1になったときC＝1が得られれば回路はすべて正常に動作をし，正しく記憶したことを表わしている。C＝1を検出してからIを$\frac{1}{2}$としてもMは前の値を保持していて，Mが0または1であればこの出力は正しく，回路に故障がないことを示し，もしMが$\frac{1}{2}$になれば故障が生じたことを表わしている。このMEMORYは clear する必要はなく，CHECK 回路をも考慮に入れれば FAIL SAFE となる。なお，第8表の状態表は，入力，出力をすべて0または1に限れば，第6表のF－Fの状態表と本質的に同じであることに注意せよ。

M ＼ I	0	$\frac{1}{2}$	1
0	⓪	⓪	$\frac{1}{2}$
$\frac{1}{2}$	0	$\frac{1}{2}$	1
1	$\frac{1}{2}$	①	①

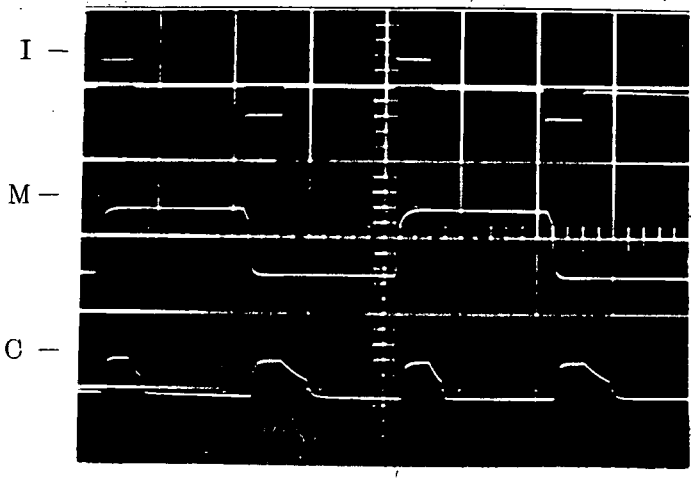
第8表　Mの状態表



第8図　特殊なFail Safe Memory の構成図

M ＼ I	0	$\frac{1}{2}$	1
0	1	$\frac{1}{2}$	$\frac{1}{2}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
1	$\frac{1}{2}$	$\frac{1}{2}$	1

第9表　Cの真理値表



第9図　動作図　　↕ 50〔V〕／cm　↔100〔μS〕／cm

この特殊なMEMORYを実際に構成し，実験した結果を第9図に示す。ここで，V＝20〔V〕とし，

ＭＥＭＯＲＹの入力があってからＣＨＥＣＫがとれるまでの時間遅れは約２０〔μＳ〕である。

Ｖ　あ　と　が　き

いくつかのＦＡＩＬ　ＳＡＦＥ　ＭＥＭＯＲＹの構成法を示した。最後に，非同期式計算機に適した特殊なＭＥＭＯＲＹについて考察し，その実験結果を示した。このＭＥＭＯＲＹではＣＨＥＣＫ出力を検出することによって回路が正常に動作しているか否かを判定することができる。

終りに，日頃ご指導，ごべんたつをいただく本学後藤以紀教授電気試験所駒宮電子部品部長に深謝する次第です。また，この研究は筆者が工業技術院電気試験所制御部自動制御研究室において，実習生として一緒に研究させていただいているもので，土屋技官に全面的に御指導を仰いだ。ここに厚くお礼を申し上げます。そして，この機会を与えて下さった上滝制御部長，佐藤自動制御室長に感謝いたします。

参　考　文　献

※１　：　土屋；フエイルセイフ論理方式の研究，昭４４年１月電気試験所研究報告　６９５号

※２　：　向殿；Ｆａｉｌ　Ｓａｆｅ　Ｓｙｓｔｅｍ，　明治大学大学院紀要　１９６６

※３　：　向殿；ＦＡＩＬ　ＳＡＦＥ　論理回路の応用，　明治大学大学院紀要　１９６７

※４　：　向殿；フエイルセイフ信号系模擬装置，明治大学大学院紀要　１９６８

※５　：　向殿，土屋，駒宮；Ｃ形フェイルセイフ論理の数学的構造について(1)，信学会電子計算機研究会資料，１９６８年５月。

※６　：　向殿，後藤；２値論理を含む３値論理関数の一考察，明治大学工学部研究報告，№２３。